



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/675,823	09/29/2000	David A. Wyatt	42390P9904	9744

7590 06/16/2005

Blakely Sokoloff Taylor & Zafman LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025

EXAMINER

SALTARELLI, DOMINIC D

ART UNIT

PAPER NUMBER

2611

DATE MAILED: 06/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/675,823	WYATT ET AL.	
	Examiner	Art Unit	
	Dominic D. Saltarelli	2611	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 17 March 2005.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-3,5-7,9-12,14-17 and 19-25 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) 4,11,16,21 and 22 is/are allowed.
 6) Claim(s) 1,2,5-7,9,12,14,17,19,20 and 23-25 is/are rejected.
 7) Claim(s) 3,10 and 15 is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____. | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Objections

1. Claim 1 is objected to because of the following informalities: Line 7 reads "ensuring unauthorized duplication" and should read --ensuring no unauthorized duplication--.
2. Claim 9 is objected to because of the following informalities: Line 19 reads "ensuring unauthorized duplication" and should read --ensuring no unauthorized duplication--.
3. Claim 14 is objected to because of the following informalities: Line 20 reads "ensuring unauthorized duplication" and should read --ensuring no unauthorized duplication--.
4. Claim 19 is objected to because of the following informalities: Line 18 reads "ensuring unauthorized duplication" and should read --ensuring no unauthorized duplication--. Appropriate correction is required.

Response to Arguments

5. Applicant's arguments with respect to claims 1-7, 9-12, 14-17, and 19-25 have been considered but are moot in view of the new grounds of rejection.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1, 7, 9, 12, 14, 17, 19, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sullivan et al. (6,069,647, of record) in view of Tsukamoto et al. (US RE38,055 E, reissue of US Patent No. 5,699,426).

Regarding claims 1 and 19, Sullivan discloses a method and article of manufacture comprising:

Selecting a protected content sink device for display of a content stream (selection of programmable unit 120, col. 2 line 64 – col. 3 line 9 and col. 3, lines 55-65);

Storing, by a content stream source application (operating system of interface unit 110, col. 3, lines 55-65 and col. 4 lines 57-65), an expected session identification code (time sensitive key, col. 3, lines 55-65) of a display content stream path from which content is received by the protected content sink device (content stream path is communication link 140, col. 4, lines 48-56);

Opening a secure connection between the content stream source application and a transmitter unit attached to the content sink device (establishment of session key, col. 8, lines 24-43, wherein the content sink device must include a transmitter unit for transmitting the received information to the internal components of the sink, col. 5, lines 45-54);

Transmitting the content stream to the transmitter unit (digital bit stream 160, col. 4, lines 35-47) along with an updated session identification code (the time sensitive key is transmitted to programmable unit 120 from interface unit

110, col. 7, lines 10-21) that is stored by the transmitter unit (programmable unit 120 also stores the TSK, col. 3, lines 55-65) and identifies a display content stream path on which the content stream was transmitted (TSK is a vital piece of information which enables the transfer of information over the content stream path, col. 3 line 66 – col. 4 line 20);

Requesting, by the content stream source application (110), the updated session identification code from the transmission unit (interface unit 110 requests the TSK back from the programmable unit 120, col. 8, lines 44-60) using a content protection protocol (communications are encrypted using the session key, col. 8, lines 24-43); and

Comparing (at interface unit 110) the updated session identification code received from the transmitter unit against the expected session identification code to ensure that the content display stream has not been routed to an unprotected content sink device (col. 8, lines 56-60).

Sullivan fails to disclose requesting, by a source application, a graphics driver to provide mode information for each content sink device attached to a graphics controller and selecting, as the protected content sink device, a content sink device implementing a content protection protocol ensuring unauthorized duplication of content displayed by the content sink device.

In an analogous art, Tsukamoto teaches requesting, by a source application, mode information for attached content sink devices and selecting a content sink device implementing a content protection protocol ensuring no

unauthorized duplication of content displayed by the content sink device (the source, receiver 21 in fig. 1, receives content and will only address content to display devices that have card keys containing the correct security key, col. 6 line 45 – col. 7 line 59, wherein only devices with the correct security keys are running a content protection protocol which ensures no unauthorized duplication of displayed content, col. 7 line 60 – col. 8 line 62), for the benefit of providing security when multiple devices are connected to a common bus (col.1, lines 50-53).

It would have been obvious at the time to a person of ordinary skill in the art to modify the method and article of manufacture disclosed by Sullivan to include requesting, by a source application, mode information for attached content sink devices and selecting a content sink device implementing a content protection protocol ensuring no unauthorized duplication of content displayed by the content sink device, as taught by Tsukamoto, for the benefit of providing enhanced security when multiple devices are connected to a common bus by discriminating among available devices when selecting a content sink.

Regarding claims 7 and 25, Sullivan and Tsukamoto disclose the method and article of manufacture of claims 1 and 19, wherein Sullivan discloses comparing the session identification code further comprises:

receiving a status word containing the updated session identification code from the transmitter unit and computing a digital signal across the status word to

verify the authenticity of the status word (communications are between 110 and 120 are encrypted, col. 8, lines 24-43, thus the requested session identification code is received as an encrypted status word, wherein the status represented by the word is in regards to the identity of 120, and successful decryption involves computing a digital signal across the word and verifies the authenticity of the status word); and

comparing the updated session identification code against the expected identification code and when the updated session identification code is not equal to the expected session identification code, discontinuing the transmission of the content stream (col. 8, lines 44-60).

Regarding claims 9 and 14, Sullivan discloses an apparatus, comprising:
A transmitter unit (fig. 1, programmable unit 120, col. 5, lines 45-54) attached to a respective display content stream path (fig. 1, communication link 140, col. 4, lines 48-56) from which content is received (content is digital bit stream 160, col. 4, lines 35-47) and stores an expected session identification code identifying the respective display content stream path attached to the transmitter unit (time sensitive key, col. 4, lines 20-34);

A graphics controller (fig. 1, interface unit 110, col. 4, lines 57-65) transmits content to the transmitter unit attached to a display content stream path (col. 4, lines 35-47) along with an updated session identification code that is stored by the transmitter unit and identifies the display content stream path on

which the content stream was transmitted (time sensitive key is sent after selecting the secure content sink, col. 7, lines 10-21, which is stored by the programmable unit, col. 7, lines 40-58);

A content sink device displays content transmitted by the graphics controller (programmable unit 120 is an output for display, col. 5, lines 45-54); and

A content source application (operating system of interface unit 110, col. 3, lines 55-65 and col. 4 lines 57-65) selects a protected content sink device (selection of programmable unit 120, col. 2 line 64 – col. 3 line 9 and col. 3, lines 55-65) for display of a content stream (digital bit stream 160, col. 4, lines 35-47), opens a secure connection with a transmitter unit attached to the protected content sink device (col. 8, lines 24-43), requests the updated session identification code from the transmission unit (col. 8, lines 44-60) using a content protection protocol (the communications are encrypted) and compares the updated session identification code against the expected identification code to ensure that the content display stream has not been routed to an unprotected content sink device (col. 8, lines 44-60);

Wherein a processor executes said instructions (fig. 2, controller 250).

Sullivan fails to disclose a graphics driver to provide mode information for each content sink device attached to the graphics controller in response to a request by the source application, such that the source application selects, as the protected content sink device, a content sink device implementing a content

protection protocol ensuring no unauthorized duplication of content displayed by the content sink device.

In an analogous art, Tsukamoto teaches requesting, by a source application, mode information for attached content sink devices and selecting a content sink device implementing a content protection protocol ensuring no unauthorized duplication of content displayed by the content sink device (the source, receiver 21 in fig. 1, receives content and will only address content to display devices that have card keys containing the correct security key, col. 6 line 45 – col. 7 line 59, wherein only devices with the correct security keys are running a content protection protocol which ensures no unauthorized duplication of displayed content, col. 7 line 60 – col. 8 line 62), for the benefit of providing security when multiple devices are connected to a common bus (col.1, lines 50-53).

It would have been obvious at the time to a person of ordinary skill in the art to modify the method and article of manufacture disclosed by Sullivan to include requesting, by a source application, mode information for attached content sink devices and selecting a content sink device implementing a content protection protocol ensuring no unauthorized duplication of content displayed by the content sink device, as taught by Tsukamoto, for the benefit of providing enhanced security when multiple devices are connected to a common bus by discriminating among available devices when selecting a content sink.

Regarding claims 12 and 17, Sullivan and Tsukamoto disclose the apparatus of claims 9 and 14, and Sullivan further discloses a digital visual output port (fig. 2, I/O port 114, col. 4 line 57 – col. 5 line 13) such that the transmitter unit is coupled to the graphics controller by the digital visual output port (col. 5, lines 11-13).

8. Claims 2 and 20 rejected under 35 U.S.C. 103(a) as being unpatentable over Sullivan and Tsukamoto as applied to claims 1 and 19 above, and further in view of Blumenau et al. (US 2003/0115324 A1, of record) [Blumenau].

Regarding claims 2 and 20, Sullivan and Tsukamoto disclose the method and article of manufacture of claims 1 and 19, wherein Sullivan discloses the interface unit (110) contains a graphics controller (fig. 2, controller 250 which controls with flow of graphics through the interface unit, col. 5, lines 28-44) but fails to disclose prior to selecting the protected content sink device:

Generating a series of session identification codes for each display content stream path supported by the graphics controller and transmitting, by the graphics controller, a session identification code to a corresponding transmitter unit from the series of identification codes for each transmitter unit attached to the graphics controller.

In an analogous art, Blumenau teaches generating a series of session identification codes for a series of connections supported by a data management system and transmitting, by the data management system, a session

identification code to a corresponding host unit from the series of identification codes for each host unit attached to the data management system (paragraph 52), further enhancing and augmenting the security of system a system which supports multiple connection paths (paragraph 51).

It would have been obvious at the time to a person of ordinary skill in the art to modify the method and article of manufacture disclosed by Sullivan and Tsukamoto to generate, prior to selecting the protected content sink device, a series of session identification codes for each display content stream path supported by a graphics controller and transmitting, by the graphics controller, a session identification code to a corresponding transmitter unit from the series of identification codes for each transmitter unit attached to the graphics controller, as taught by Blumenau, for the benefit of providing enhanced security over multiple connection paths (such as interface unit 110 acting as a home gateway for several programmable devices 120 throughout a home).

9. Claims 5, 6, 23, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sullivan and Tsukamoto as applied to claims 1 and 19 above, and further in view of Ming et al. (5,710,815, of record) [Ming].

Regarding claims 5 and 23, Sullivan and Tsukamoto disclose the method and article of manufacture of claims 1 and 19, and Sullivan additionally discloses receiving, by a graphic controller (fig. 1, interface unit 110, includes a graphic controller for facilitating the transmission of the digital bit stream, col. 4, lines 35-

47), the content stream from the content stream source application for display on the protected content sink device (the graphic controller will forward the content stream through output port 114 for delivery to the display device, col. 4 line 57 – col. 5 line 13).

Sullivan and Tsukamoto fail to disclose transmitting the updated session identification code to the transmission unit during a vertical blanking interval (VBI) in the content stream, detecting, by the transmission unit, a VBI signal within the content stream, latching, by the transmission unit, the updated session identification code when the VBI is detected, and repeating the transmitting, detected, and latching steps for a duration of the content stream.

In an analogous art, Ming teaches inserting authorization information (access control data, col. 6, lines 6-15) into the VBI of a content stream (col. 6, lines 16-29) repeatedly, for the duration of the content stream (the access control data is found within every video frame, col. 7, lines 22-30), for the benefit of maintaining an on-going access control scheme using an otherwise unused and unobtrusive section of a content stream.

It would have been obvious at the time to a person of ordinary skill in the art to modify the method and article of manufacture of Sullivan and Tsukamoto to include repeatedly inserting the updated session identification information in the VBI of the content stream, which inherently includes detecting and subsequently latching the updated session identification code during the VBI in order to retrieve

it, as taught by Ming, for the benefit of maintaining the access control scheme using an otherwise unused and unobtrusive section of a content stream.

Regarding claims 6 and 24, Sullivan and Tsukamoto disclose the method and article of manufacture of claims 1 and 19, but fail to disclose performing the transmitting, requesting, and comparing after a predetermined period of time and repeating the performing while the content stream is displayed on the protected content stream device.

In an analogous art, Ming teaches utilizing access control information to restrict access to content streams on an on-going basis (access control information is within every frame of video data, col. 7, lines 22-30) granting access control over live broadcast streams (col. 6 line 59 – col. 7 line 30), negating the possibility of an unauthorized user from simply waiting till after authorization information has been sent before attempting to access a content stream.

It would have been obvious at the time to a person of ordinary skill in the art to modify the method and article of manufacture disclosed by Sullivan and Tsukamoto to include utilizing the session identification codes to control access to content streams on an on-going basis, as taught by Ming, for the benefit of maintaining content sink verification in a on-going manner.

Allowable Subject Matter

10. Claims 4, 11, 16, 21, and 22 are allowed.
11. Claims 3, 10, and 15 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

12. The following are suggested formats for either a Certificate of Mailing or Certificate of Transmission under 37 CFR 1.8(a). The certification may be included with all correspondence concerning this application or proceeding to establish a date of mailing or transmission under 37 CFR 1.8(a). Proper use of this procedure will result in such communication being considered as timely if the established date is within the required period for reply. The Certificate should be signed by the individual actually depositing or transmitting the correspondence or by an individual who, upon information and belief, expects the correspondence to be mailed or transmitted in the normal course of business by another no later than the date indicated.

Certificate of Mailing

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

on _____
(Date)

Typed or printed name of person signing this certificate:

Signature: _____

Certificate of Transmission

I hereby certify that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office, Fax No. (703) _____ - _____ on _____.
(Date)

Typed or printed name of person signing this certificate:

Signature: _____

Please refer to 37 CFR 1.6(d) and 1.8(a)(2) for filing limitations concerning facsimile transmissions and mailing, respectively.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dominic D. Saltarelli whose telephone number is (571) 272-7302. The examiner can normally be reached on Monday - Friday 7:00am - 4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Christopher Grant can be reached on (571) 272-7294. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Dominic Saltarelli
Patent Examiner
Art Unit 2611

DS



HALTRAN
PRIMARY EXAMINER